Amendments to the Claims:

This listing of claims will replace all prior versions, and listing, of claims in the application:

Listing of Claims:

1. (currently amended) A system for detecting and responding to an attack, comprising:

a first device attached to a network and configured to:

detect an attack based on received traffic,

create attack information, and

forward the attack information to the network using a link state routing protocol or a path vector routing protocol; and

a second device configured to receive the attack information and detect particular traffic based on the attack information.

2. (original) The system of claim 1, wherein the first device comprises a firewall filter.

3. (original) The system of claim 1, wherein the first device comprises:

a filter device configured to perform stateful filtering.

4. (currently amended) The system of claim 1, wherein the first device comprises:

a packet generating element configured to generate a link state routing packet that ~~include~~ includes the attack information.

5. (original) The system of claim 1, wherein the second device comprises a router.

6. (currently amended) The system of claim 1, wherein the first device ~~uses a distributed routing protocol for sending~~ forwards the attack information using a path vector routing packet.

7. (canceled)

8. (canceled)

9. (original) The system of claim 1, wherein the second device forwards the attack information to other devices.

10. (original) The system of claim 1, wherein the second device configures a filter based on the attack information.

11. (original) The system of claim 1, wherein the second device uses the attack information for a predetermined amount of time.

12. (original) The system of claim 1, wherein the second device rate limits the particular traffic.

13. (original) The system of claim 1, wherein the second device counts the particular traffic.

14. (currently amended) A method of detecting and responding to an attack, comprising:

detecting an attack at a first device based on incoming traffic;

generating attack information defining characteristics of the attack;

sending the attack information to a second device in a network using at least one of a link state routing packet or a path vector routing packet; and

detecting traffic at the second device based on the attack information.

15. (original) The method of claim 14, including:

configuring the first device to detect traffic based on the detected attack.

16. (canceled)

17. (original) The method of claim 14, wherein the sending includes:

sending the attack information using a distributed routing protocol.

18. (original) The method of claim 14, wherein the sending includes:

sending the attack information using a link state routing protocol.

19. (original) The method of claim 14, further including:

authenticating the attack information at the second device.

20. (original) The method of claim 14, further including:

sending the attack information from the second device to another device.

21. (original) The method of claim 14, further including:

monitoring the attack at the second device.

22. (original) The method of claim 14, further including:

detecting traffic based on the attack information for a particular period of time.

23. (original) The method of claim 14, further including:

rate limiting traffic that matches attack characteristics defined in the attack information.

24. (original) The method of claim 14, wherein the sending includes:

sending the attack information using one of a markup language or hypertext protocol.

25. (currently amended) A device for detecting an attack, comprising:

an attack detection element configured to detect an attack in incoming traffic;

an attack information generator configured to generate attack information defining characteristics of the attack; and

a transmitting element configured to transmit the attack information to a device on a network using at least one of a link state routing protocol or a path vector routing protocol.

26. (original) The device of claim 25, further comprising:

a filter element configured to filter incoming traffic and forward filter information to the attack detection element.

27. (original) The device of claim 26, wherein the attack information generator is further configured to send attack information to the filter element.

28. (original) The device of claim 25, wherein the transmitting element is further configured to transmit the attack information using a distributed routing protocol.

29. (currently amended) The device of claim 25, wherein the transmitting element is ~~further~~ configured to transmit the attack information using a link state routing protocol.

30. (original) The device of claim 25, wherein transmitting element is further configured to transmit the attack information using an authentication mechanism.

31. (original) The device of claim 25, wherein the transmitting element is further configured to transmit the attack information using encryption.

32. (original) The device of claim 25, wherein the attack is a denial of service attack.

33. (currently amended) A method of detecting an attack, comprising:

monitoring incoming traffic at a first device to detect an attack;

generating attack information defining characteristics of the attack; and

transmitting the attack information to a second device via a network using a link state routing protocol, a path vector routing protocol, a markup language protocol or a hypertext protocol.

34. (original) The method of claim 33, wherein the attack is a denial of service attack.

35. (original) The method of claim 33, wherein the monitoring includes:

using information from a filter to detect the attack.

36. (original) The method of claim 33, wherein the generating includes:

sending attack information to a filter for configuring the filter based on the attack.

37. (original) The method of claim 33, further including:

performing stateful filtering on incoming traffic.

38. (original) The method of claim 33, wherein the transmitting includes:

sending the attack information in a packet.

39. (canceled)

40. (original) The method of claim 33, wherein the transmitting includes:

sending the attack information using a link state routing protocol.

41. (original) The method of claim 33, wherein the transmitting includes:

sending the attack information using a markup language protocol or a hypertext protocol.

42. (original) The method of claim 33, wherein the transmitting includes:

sending the attack information in a secure format.

43. (currently amended) A device for responding to an attack, comprising:

a receiver configured to receive attack information from a first device that sent the attack information; ~~and~~

a configuration element configured to configure a second device based on the received attack information; and

a transmitting element for transmitting the attack information to another device using a link state routing protocol, a path vector routing protocol, a markup language protocol or a hypertext protocol.

44. (canceled)

45. (original) The device of claim 43, wherein the configuration element comprises:

a filter; and

an attack configuration generator.

46. (original) The device of claim 43, wherein the configuration element is further configured to configure the second device based on filter information.

47. (original) The device of claim 43, wherein the configuration element is further configured to unconfigure the second device after a predetermined period of time after configuring based on the attack information.

48. (original) The device of claim 43, wherein the second device comprises a router.

49. (original) The device of claim 43, wherein the configuration element is further configured to authenticate the received attack information.

50. (original) The device of claim 43, wherein the configuration element is further configured to detect particular traffic based on the attack information.

51. (original) The device of claim 43, wherein the configuration element is further configured to monitor traffic and send monitoring results to the first device.

52-60. (canceled)

61. (currently amended) A method for responding to an attack, comprising:

receiving attack information at a central management system from a first device via a network;

managing a response to the attack at the central management system;

receiving, at the central management system, additional attack information from other devices via the network; and

communicating, by the central management system, information associated with the additional attack information to the first device.

62. (original) The method of claim 61, wherein the managing includes:

sending the attack information to other devices via a network.

63. (canceled)

64. (original) The method of claim 61, wherein the managing includes:

collecting information related to the attack information.